Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement für Verteidigung,
Bevölkerungsschutz und Sport VBS

Bundesamt für Cybersicherheit BACS

7. März 2024

Bericht zu den Datenanalysen nach dem Cyberangriff auf die Firma Xplain

Inhalt

1 Einleitung

Der Ransomware-Angriff auf die Firma Xplain, welche ein wichtiger Dienstleister verschiedener Stellen der Bundesverwaltung und einiger Kantone ist, hat zum Abfluss von grossen Mengen an Informationen geführt. Betroffen waren auch sicherheitsrelevante und personenbezogene Daten, insbesondere aus dem Bereich der inneren Sicherheit. Die Angreifer haben die Daten im Darknet publiziert, womit diese Daten öffentlich einsehbar wurden.
Die Veröffentlichung vertraulicher und sicherheitsrelevanter Daten hat gravierende Auswirkungen und führt zu grossen Aufwänden. Es mussten Sofortmassnahmen identifiziert und umgesetzt werden, um die unmittelbaren Risiken einzudämmen und Betroffene zu informieren. Es musste zudem beurteilt werden, ob Systeme und Datenbanken der Bundesverwaltung kompromittiert wurden. Zudem mussten Massnahmen umgesetzt werden, damit die Systeme überhaupt wieder betrieben werden können. Diese Arbeiten dauern teilweise immer noch an.
Der Vorfall führte dazu, dass wichtige Systeme nicht mehr eingesetzt werden konnten. Zudem war ein hoher personeller Aufwand zu seiner Bewältigung nötig. Neben diesen unmittelbaren Auswirkungen entstand dem Bund ein zusätzlicher Schaden, weil das Vertrauen in die Sicherheit der Datenbearbeitung durch den Bund beeinträchtigt ist. Es ist schwer einzuschätzen ob und wie sich ein solcher Vertrauensverlust auswirkt, sicher ist aber, dass der Bund alles unternehmen muss, um sich das Vertrauen wieder zu erarbeiten.
Dazu gehört als erster Schritt eine umfassende Aufarbeitung des Vorfalls. Der Bundesrat hat sich bereits dazu entschieden, diese Analyse anzugehen und hat am 23. August 2023 eine Administrativuntersuchung angeordnet. Diese soll aufzeigen, ob die Bundesverwaltung bei der Auswahl, Instruktion und Überwachung der Xplain AG sowie der Zusammenarbeit mit dieser Firma ihre Pflichten angemessen erfüllt hat. Zudem sollen Massnahmen identifiziert werden, um einen ähnlichen Vorfall künftig zu verhindern. Die Administrativuntersuchung soll bis Ende März 2024 abgeschlossen werden. Nach deren Durchführung wird der Bundesrat über die Ergebnisse und Empfehlungen informiert, damit er über die Folgen der Administrativuntersuchung entscheiden kann.
Das Nationale Zentrum für Cybersicherheit (NCSC), das heutige Bundesamt für Cybersicherheit (BACS), hat die Vorfallbewältigung geleitet, hat Massnahmen zur Wiederherstellung der Sicherheit der Systeme definiert und eine umfassende Analyse der veröffentlichten Daten durchgeführt. Als Beitrag zur Aufarbeitung des Vorfalls und zur Schaffung einer grösstmöglichen Transparenz publiziert es den vorliegenden Bericht über das Vorgehen und die Resultate der Datenanalyse. Ziel ist es, einen Überblick zu geben, welche Art von Daten betroffen war und die Herausforderungen bei der Datenanalyse zu beschreiben.
Eine wichtige Frage betrifft dabei auch die Menge der publizierten Daten. Die Angreifer selber haben zunächst kommuniziert, über insgesamt 907 GB Daten zu Verfügen. Publiziert haben sie aber anschliessend nur ca. 400 GB. Es stand deshalb die Frage im Raum, ob die Angreifer Daten bewusst nicht veröffentlicht haben oder ob ihre initialen Angaben nicht korrekt waren. Es ist wichtig, diese Frage beurteilen zu können, damit das Risiko abgeschätzt werden kann, ob weitere Erpressungen erfolgen oder die Daten durch die Angreifer anderweitig weitergegeben wurden. Im Bericht wird aufgezeigt, wie diese Frage analysiert wurde und warum das NCSC in Rücksprache mit den betroffenen Stellen und dem NDB zum Schluss kommt, dass kein hohes Risiko dafür besteht, dass die Angreifer bewusst nicht alle erbeuteten Daten veröffentlicht haben.
Wichtig zu betonen ist, dass der vorliegende Bericht keine inhaltliche Bewertung der Datenbestände vornimmt und auch nicht analysiert, weshalb welche Daten abfliessen konnten. Diese Fragen werden ausschliesslich in den laufenden Verfahren zum Vorfall, insbesondere im Rahmen der Administrativuntersuchung geklärt.

2 Ausgangslage

«Double Extortion»-Ransomware ist eine Variante der Ransomware-Angriffe, bei der Angreifer zusätzlich zur Verschlüsselung von Daten auch drohen, gestohlene Informationen zu veröffentlichen, um Lösegeld zu erpressen. Opfer müssen zahlen, um sowohl ihre Daten zu entschlüsseln als auch die Veröffentlichung sensibler Informationen zu verhindern. Die Anzahl solcher Fälle hat sowohl in der Schweiz als auch international stark zugenommen.
Ende Mai 2023 hat eine unter dem Namen «Play» auftretende Hackergruppierung einen solchen Ransomware-Angriff gegen die auf IT-Lösungen im Bereich der inneren Sicherheit spezialisierte Firma Xplain AG durchgeführt. Sie hat dabei grosse Datenmengen gestohlen und gedroht, diese zu veröffentlichen. Da Xplain sich in Absprache mit den Strafverfolgungsbehörden und dem Bund nicht erpressen liess und keine Lösegeldzahlung an die Hacker leistete, veröffentlichten diese am 14. Juni 2023 die entwendeten Daten im Darknet. Die Bundesverwaltung als Kunde von Xplain war von diesem Cybervorfall ebenfalls betroffen. Die betroffenen Stellen setzten Sofortmassnahmen um, um das Risiko für die Bundesverwaltung und betroffene Dritte zu minimieren. Das NCSC leitete gestützt auf Art. 12 Abs. 5 der Cyberrisikenverordnung die verschiedenen operativen Arbeiten im Rahmen der Vorfallsbearbeitung und führte Analysen der veröffentlichten Daten im Darknet durch.
Für die Bundesverwaltung stellten sich zu Beginn des Vorfalls verschiedene Herausforderungen. Insbesondere war unklar, welche Daten genau bei der Firma Xplain entwendet wurden, und um welche Datenmenge es sich konkret handelte. Des Weiteren war ungewiss, welche Einheiten der Bundesverwaltung in welchem Ausmass betroffen waren. Ohne Sichtung und Analyse der publizierten Daten war eine Einschätzung des Risikos und des potenziellen Schadensausmasses für die Bundesverwaltung nicht möglich.
Aus praktischer und operativer Sicht gestaltete sich bereits der Zugriff auf die Daten als sehr aufwändig, da der Datenbestand nur sehr langsam aus dem Darknet heruntergeladen werden konnte und dieser Vorgang zwischenzeitlich auch immer wieder unterbrochen wurde. Es erforderte einige Tage, bis der komplette Datensatz heruntergeladen war und zur Analyse bereitstand. Nun bestand die Herausforderung darin, diese Daten forensisch zu analysieren. Dies ist bei grossen Mengen an unstrukturierten Daten – wie sie in diesem Fall vorlagen – aus folgenden Gründen besonders herausfordernd:

- Unterschiedliche Datenformate: Unstrukturierte Daten können in vielen Formen vorliegen, z. B. Textdokumente, E-Mails, Bilder, Videos, Audioaufnahmen oder technische Formate. Jedes dieser Formate erfordert spezielle Tools und Kenntnisse für die Analyse. Im Xplain Datendump waren verschiedene Datenformate enthalten, welche nicht direkt lesbar waren. Diese mussten zuerst bearbeitet und aufbereitet werden, damit der Inhalt verständlich und interpretierbar war.
- Relevanz der Daten: Bei grossen Datenmengen ist es generell eine Herausforderung, relevante von irrelevanten Informationen zu unterscheiden. Beim Xplain Datendump musste zunächst festgestellt werden, welche Daten für die Bundesverwaltung relevant waren und welche nicht.
- Tools, Ressourcen und Know-how: Eine grosse Datenmenge kann nicht manuell und ohne entsprechende Werkzeuge analysiert werden. Die notwendigen Tools und Ressourcen für die Analyse unstrukturierter Daten können aber teuer sein, ebenso ist für die Bedienung der nötigen Tools entsprechendes Fachwissen erforderlich.

3 Ziele der Datenanalyse der Bundesverwaltung

Der politisch-strategische Krisenstab «Datenabfluss» (PSK-D) [1] hat das NCSC beauftragt, eine Analyse des Datenbestands vorzunehmen. Die Analyse basierte auf zwei Schritten: In einem ersten Schritt erfolgten die systematische Kategorisierung und Triage aller relevanten Dokumenten. In einem zweiten Schritt wurden die wichtigsten Resultate und Ergebnisse von den verschiedenen Stellen innerhalb der Bundesverwaltung zusammengetragen und abgeglichen.

Die erste Triage und Sichtung hatten zum Ziel, die folgenden Fragen zu beantworten:

- Welche Verwaltungseinheiten sind in welchem Ausmass betroffen;
- Welche Risiken entstehen dem Bund durch die Veröffentlichung;
- Wie viele klassifizierte Informationen wurden veröffentlicht;
- Wie viele Dokumente enthalten Personendaten;
- Welche weiteren Erkenntnisse ergeben sich aus den Datenanalysen.

Im zweiten Schritt ging es darum den unmittelbaren und mittelbaren Handlungsbedarf festzustellen. Daten mit einem unmittelbaren Handlungsbedarf wurden den zuständigen Stellen sofort übergeben. Alle übrigen relevanten Daten wurden den jeweiligen Verwaltungseinheiten nach Abschluss der Triage zur weiteren Prüfung übergeben. Eine abschliessende inhaltliche Bewertung und Risikoabschätzung sind jeweils nur durch den Eigentümer der Daten respektive durch die verantwortliche Verwaltungseinheit möglich. Im Rahmen der Vorfallsbearbeitung hat das NCSC die Triage von Informationen in enger Zusammenarbeit mit anderen Behörden und betroffenen Organisation wahrgenommen, insbesondere mit fedpol, den Kantonen, dem Netzwerk digitale Ermittlungsunterstützung Internetkriminalität (NEDIK) sowie mit Betreibern kritischer Infrastrukturen.
Zudem hat das NCSC Anfragen aus der Öffentlichkeit koordiniert und bei Anfragen Suchläufe im Datenbestand durchgeführt, damit die zuständigen Bundesstellen Auskunft darüber erteilen konnten, ob die Anfragenden von der Datenveröffentlichung betroffen sind oder nicht.

4 Beschreibung der veröffentlichten Daten

Gegenstand der Analyse ist der durch die Täterschaft Play im Darknet veröffentlichte Datensatz. Bei der Bewältigung des Sicherheitsvorfalls unter der Leitung des NCSC haben die verschiedenen betroffen Bundesämter und Leistungserbringer eng zusammengearbeitet. Dadurch konnten Synergien genutzt, Ressourcen sinnvoll eingesetzt und wertvolle Zeit gewonnen werden.
Veröffentlicht wurden im Darknet insgesamt 646 RAR-Archivdateien, jeweils ca. 500 MB und eine Datei mit der Grösse 385 MB. Das gesamte Datenvolumen der komprimierten Archivdaten umfasste Total 339 GB. Die Dateien waren in verschlüsselter Form abgelegt, das Passwort zur Entschlüsselung wurde ebenfalls durch die Täterschaft Play auf der Leak-Seite veröffentlicht. Entpackt handelte es sich um die Datenmenge von 431 GB, darin enthalten 146’623 Dateien und 19’863 Ordner.
Die Angaben von Datenmengen dienen zur Einschätzung des Ausmasses der veröffentlichten Daten. Es handelt sich nicht um genaue und abschliessende Zahlen, da Mengenangaben zu Daten unterschiedlich interpretiert werden können und daher nicht immer vergleichbar sind. Je nachdem, wie Dateien oder Dokumente gezählt werden, ob z. B. in komprimierter oder entpackter Form, ergeben sich unterschiedliche Datengrössen und Mengenangaben.

[1] https://www.ncsc.admin.ch/ncsc/de/home/aktuell/im-fokus/2023/xplain_3.html

In einer kompromittierten ZIP-Datei können mehrere weitere Dateien enthalten sein, z. B. verschiedene E-Mails. Jede dieser E-Mail beinhaltet weitere Anhänge wie Word- oder PowerPoint-Dokumente. In diesen Office-Dokumenten wiederum können weitere Objekte wie Bilder, Videos eingebettet sein. Wir sprechen daher im Rahmen dieser Analyse von Objekten, damit können sowohl einzelne Dateien aber auch die darin enthalten Objekte gemeint sein.
Das weitere Vorgehen hatte zum Ziel, die Gesamtmenge der für die Bundesverwaltung relevanten Daten zu identifizieren, um die Analyse und Auswertung möglichst effizient zu gestalten. Der Datenbestand enthielt verschiedene Sicherungskopien von Servern der Firma Xplain (zwei Dateien, 260 GB) sowie weitere Datenbestände ohne Relevanz für die Bundesverwaltung. Dabei handelte es sich primär um Systemdateien, Programme oder Standartkomponenten, welche z. B. für die Softwareentwicklung eingesetzt werden. Diese können durch den automatisierten Abgleich mittels Prüfsummen von Referenz-Datenbeständen (sogenannte Hash-Listen) ausgeschlossen werden.
Die System- und Backupdateien wurden automatisiert und mittels Stichwortsuchen überprüft und von der weiteren Analyse ausgeschlossen. Der Restdatenbestand, welcher als relevant für die Bundesverwaltung eingestuft wurde, umfasste ca. 65'000 Dokumente und wurde in der Folge einer weiterführenden manuellen Prüfung und Sichtung unterzogen. Die im nachfolgenden Kapitel 6 beschriebene Datenauswertung bezieht sich somit auf die relevante Teildatenmenge der ca. 65'000 Dokumente, die vom gesamten veröffentlichen Datenbestand ca. 5% umfassen.

	Anzahl Objekte	**Prozent**
Gesamter Datenbestand	1'295'862	100
Duplikate	830'894	64
Nicht relevant (Backup, Systemdateien, Standardkomponenten)	401’717	31
Relevant: Manuelle Prüfung und Visionierung	**64’793**	**5**

Tabelle 1 Übersicht Datenbestand

5 Datenauswertung

Bei der Analyse grosser Datenmengen werden sogenannte eDiscovery-Systeme eingesetzt. Diese ermöglichen eine effiziente und strukturierte Aufbereitung und Sichtung der Datenbestände. Sie verfügen auch über umfangreiche Suchfunktionen, die es erlauben, aus einer grossen Menge elektronischer Daten schnell die relevanten Informationen zu extrahieren. Ohne solche Instrumente wäre eine Datenprüfung sehr zeitaufwändig und fehleranfällig. Im Rahmen der Xplain Untersuchung hat das NCSC die bundesinterne eDiscovery-Lösung der Eidgenössische Steuerverwaltung (ESTV) eingesetzt. Diese professionelle Infrastruktur ermöglichte eine unverzügliche Aufnahme der Analysetätigkeit und eine dezentrale und virtuelle Analyse und Visionierung der Daten innerhalb der Bundesverwaltung.
Über diese eDiscovery Anwendung wurden die ca. 65'000 Dokumente manuell gesichtet und anhand einer vordefinierten Liste kategorisiert. War die Einteilung und Einschätzung nicht eindeutig, wurde in einer zweiten Runde ein Teil der Dokumente von einer zweiten Person beurteilt (4-Augen-Prinzip). Dies war in ca. 10% der Dokumente der Fall.
Im Datenbestand befanden sich auch verschiedene Datenformate und digitale Artefakte, welche nicht direkt lesbar und interpretierbar waren. Diese mussten zuerst in eine verständliche Form gebracht werden, entweder mit der dazu passenden Software oder über selber entwickelte technische Hilfsmittel. Beispiele solcher Artefakte sind Protokolldateien, Fehlermeldungen und -aufzeichnungen, Datenbank Dumps, Software-Code, Systemkonfigurationen, codierte (encoded) Bilder- und Dokumentformate, Speicher-Abbilder, verschlüsselte oder Passwort geschützte Daten, Backups verschiedener Formate und Produkte.

Bei der Datenanalyse haben zu Beginn neun Mitarbeitende aus dem NCSC mitgewirkt. Das Reviewer Team wurde zusätzlich unterstützt von weiteren 27 freiwilligen Mitarbeitenden aus zehn verschiedenen Bundesämtern. Die 36 Reviewer haben für den Review ca. 1000 Arbeitsstunden aufgewendet, wobei die meisten Reviewer nur mit einem Teilzeitengagement mitgearbeitet haben. Die Bundesangestellten, die das NCSC bei der Datenanalyse vorübergehend im Rahmen der Amtshilfe unterstützten, galten bei ihrer Tätigkeit für das NCSC als dessen Hilfspersonen und haben Geheimhaltungsvereinbarungen unterzeichnet über die Verwendungen von Informationen aus der Datenanalyse.

6 Ergebnisse der Datenanalyse

Da sowohl das Herunterladen als auch die Analyse des veröffentlichten Datensatzes mit hohem Aufwand verbunden ist, fehlte in einer ersten Phase ein Überblick darüber, wer in welchem Ausmass betroffen ist. Es war deshalb das Ziel der Datenanalyse, einen solchen Überblick zu schaffen.
Bei der Beurteilung der Betroffenheit und Verantwortlichkeit der veröffentlichten Daten wurde unterschieden zwischen *Dateneigentümer* und *betroffenen Verwaltungseinheiten*. Der Dateneigentümer ist der Herausgeber oder die verantwortliche Organisation eines Dokuments oder Datensatzes. Dies ist jeweils immer eine einzige Stelle oder Organisation. Demgegenüber können Organisationen auch von der Veröffentlichung von Dokumenten oder Datensätzen betroffen sein, obwohl sie selbst nicht Eigentümer derjenigen sind. Dies ist beispielsweise dann der Fall, wenn eine oder auch mehrere verschiedenen Organisationen in einem Dokument erwähnt werden. Ein weiteres Beispiel ist die Durchführung eines gemeinsamen Projektes mit verschiedenem Beteiligen, wie im Falle von Xplain mit Beteiligten aus der Bundesverwaltung und Kantonen. Betroffene Stellen wurden jeweils durch das NCSC direkt oder via Partnerorganisation informiert, werden aber in diesem Bericht nicht weitergehend erläutert.
In der Tabelle 2 ist die Anzahl der Objekte und der prozentuale Anteil in Bezug auf die Gesamtheit der relevanten Objekte aufgeführt: Die meisten Objekte mit einem Anteil von über 70% gehören der Firma Xplain. Etwa 14% der untersuchten Daten gehören der Bundesverwaltung, und der Anteil der Objekte der Kanton beläuft sich auf ca. 10%. Die Daten-Objekte von privaten Organisationen sowie Polizei-Korps machen jeweils weniger als 2% am Datenbestand aus. Nur vereinzelte Objekte konnten den bundesnahen Betrieben sowie der Bundesanwaltschaft zugeordnet werden (jeweils weniger als 1%)

Dateneigentümer	**Anzahl Objekte**	**Prozent**
Xplain	47413	73.03
Bundesverwaltung	9040	13.92
Kantone	6200	9.55
Private	955	1.47
Polizei	944	1.45
Bundesnahe Betriebe	355	0.55
Bundesanwaltschaft	16	0.02
Total relevante Objekte	**64’923**	**100.00**

Tabelle 2 Übersicht betroffene Dateneigentümer

In der Tabelle 3 sind die 9040 relevanten Objekte der Bundesverwaltung den Departementen zugeordnet. Daraus ist ersichtlich, dass mit 95% der grösste Anteil der relevanten Objekte den Verwaltungseinheiten des Eidgenössischen Justiz- und Polizeidepartements (EJPD) (Bundesamt für Justiz, Bundesamt für Polizei, Staatssekretariat für Migration und dem internen Leistungserbringer ISC-EJPD) gehören. Das Eidgenössische Departement für Verteidigung, Bevölkerungsschutz und Sport (VBS) ist mit etwas mehr als 3% der Daten leicht betroffen, die übrigen Departemente nur marginal.

Die hier als Dateneigentümer aufgeführten und betroffenen Verwaltungseinheiten müssen nicht zwingendermassen Kunden der Firma Xplain sein oder eine Geschäftsbeziehung mit der Firma Xplain eingegangen sein. Es ist auch möglich, dass die Daten der Verwaltungseinheiten über Dritte zu Xplain gelangt und somit im veröffentlichten Datenbestand erschienen sind. Dritte können beispielsweise andere Verwaltungseinheiten der Bundesverwaltung oder auch kantonale Behörden sein, welche untereinander Daten ausgetauscht oder gemeinsame Projekte geführt haben.

Dateneigentümer	**Anzahl Objekte**	**Prozent**
EJPD (BJ, fedpol, ISC-EJPD, SEM)	8603	95.17
VBS (Militärpolizei, NDB)	306	3.38
WBF (SECO)	69	0.76
EFD (BAZG, ISB[2], BBL, BIT)	55	0.61
EDI (BFS)	6	0.07
EDA	1	0.01
Total relevante Objekte Bundesverwaltung	**9040**	**100.00**

Tabelle 3 Betroffene Dateneigentümer der Bundesverwaltung

In der Tabelle 4 sind die total 9040 relevanten Objekte der Bundesverwaltung nach sensitiven Kriterien wie Personendaten, technische Informationen, klassifizierte Informationen und Passwörter kategorisiert. Insgesamt wurden 5182 Objekte mit sensitivem Inhalt gefunden. Bei Personendaten handelt es sich um Objekte mit identifizierenden Angaben zu natürlichen Personen wie Name, E-Mail, Telefonnummer, Adresse, usw. Etwas mehr als die Hälfte der relevanten 9040 Objekte der Bundesverwaltung enthielten Personendaten, womit diese Datenkategorie den grössten Anteil (über 90%) der sensitiven Objekte ausmacht. Unter technische Informationen fallen Beschreibungen oder Dokumentationen von IT-Systemen, Anforderungsdokumente zu Applikationen oder Architekturbeschreibungen. Die Kategorie Passwörter beinhalten Zugangsdaten, API-Keys, kryptographische Zertifikate, usw. Klassifizierte Informationen umfassen Informationen mit dem Klassifizierungsvermerk INTERN, VERTRAULICH oder GEHEIM gemäss Informationsschutzverordnung, ISchV[3]

Datenkategorie	**Anzahl Objekte**	**Prozent**
Personendaten	4779	92.22
Technische Informationen	278	5.36
Klassifizierte Informationen	121	2.34
Passwörter	4	0.01%
Total sensitive Objekte Bundesverwaltung	**5182**	**8.00%**

Tabelle 4 Sensitive Daten der Bundesverwaltung

[2] Informatikstrategieorgan Bund ISB, existiert heute nicht mehr

[3] https://www.fedlex.admin.ch/eli/cc/2007/414/de

Die Aufschlüsselung der 121 klassifizierten Objekte nach Klassifizierungsstufen ergibt folgendes Bild: Die Mehrheit der klassifizierten Daten, insgesamt 84 Objekte, sind als INTERN eingestuft. Etwa ein Drittel der Objekte sind als VERTRAULICH eingestuft. GEHEIM klassifizierte Objekte wurden keine gefunden.

Klassifikation	**Anzahl Objekte**	**Prozent**
INTERN	84	69.42
VERTRAULICH	37	30.57
GEHEIM	0	0.00
Total klassifizierte Objekte	**121**	**100.00**

Tabelle 5 Anzahl klassifizierter Daten nach Stufe

Bei der Aufteilung der sensitiven Objekte nach Verwaltungseinheit zeigt sich, dass die Mehrheit der sensitiven Objekte die Verwaltungseinheiten des EJPD betreffen.

Dateneigentümer	**Personendaten**		**Technische Informationen**		**Klassifizierte Informationen**		**Passwörter**	
	N	**%**	**N**	**%**	**N**	**%**	**N**	**%**
EJPD (BJ, fedpol, ISC-EJPD, SEM)	4644	97.2	218	78.4	87	71.9	2	50
VBS (Militärpolizei, NDB)	76	1.5	22	7.9	24	19.8	0	0
WBF (SECO)	31	0.7	26	9.4	9	7.5	2	50
EFD (BAZG, ISB, BBL, BIT)	27	0.6	10	3.6	1	0.8	0	0
EDI (BFS)	0	0	2	0.7	0	0	0	0
EDA	1	0	0	0	0	0	0	0
Total sensitive Objekte pro Kategorie	**4779**	**100.0**	**278**	**100.0**	**121**	**100.0**	**4**	**100.0**

Tabelle 6 Sensitive Daten der Bundesverwaltung nach Verwaltungseinheit

Bei den 3858 Objekten der Bundesverwaltung, welche als nicht sensitiv eingestuft wurden, handelt es sich um eine Vielzahl unterschiedlicher Datentypen wie beispielsweise E-Mail-Kommunikation, Dokumentationen von IT-Systemen, Software-Sourcecode, Projektbezogene Unterlagen, Fehlerbeschreibungen, Support-Anfragen, Screenshots von Applikationen, usw.

7 Analyse des Deltas zwischen den veröffentlichten und den gefährdeten Daten

Die Gruppe «Play» behauptete auf ihrer Internetseite, dass sie 907 GB[4] an Daten bei Xplain AG entwendet und in der Folge publiziert hätten. Es wurden jedoch nur ca. 400 GB im Darknet veröffentlicht. Diese Diskrepanz konnte nicht erklärt werden und gab zur Sorge Anlass, dass weitere Veröffentlichungen möglich sind oder die Kriminellen Teile des Datensatzes anderweitig weitergegeben haben.
Im Juli 2023 hat der politisch-strategischen Krisenstab «Datenabfluss» (PSK-D) das NCSC deshalb beauftragt, eine Analyse der Differenz zwischen den veröffentlichten und den gefährdeten Daten von Xplain durchzuführen.

[4] Im Februar 2024 korrigierte die Täterschaft die Datenmenge auf 600 GB.

Dazu nötig war ein systematischer Vergleich der bei der Firma Xplain zum Zeitpunkt des Angriffs abgelegten Datenbestände mit den veröffentlichten Daten. Die Firma Xplain hat den betroffenen Kunden aus der Bundesverwaltung die strukturiert abgelegten Datenbestände aus dem Backup übermittelt.
Die Verwaltungseinheiten stellten dem NCSC entweder diese Backup-Daten zur Verfügung, damit die Analyse durch das NCSC gemacht werden konnte, oder die Verwaltungseinheiten führten die Auswertung selbst durch und informierten das NCSC über das Ergebnis.
Das NCSC hat Datenbestände von BJ, ISC-EJPD, SEM und BAZG zur Analyse erhalten, die Auswertung der Datenbestände von fedpol und armasuisse/Militärpolizei erfolgte durch die Verwaltungseinheiten selbst.

7.1 Ergebnisse der Analysen

Diese Analysen führten zu folgenden Ergebnissen:

- Fedpol: Anhand des Abgleichs des eindeutigen Hash-Wertes von jeder Datei der 70GB Restore-Daten von fedpol zum veröffentlichen Datensatz konnte fedpol feststellen, dass ausschliesslich 39% (52’468 Files) der fedpol Daten veröffentlicht wurden. Vereinzelt fehlen in den fünf veröffentlichen Kundenprojekte Dateien und Unterverzeichnisse. In sechs Verzeichnissen konnte eine Differenz von (- 1 Datei) Anzahl nicht veröffentlichten Dateien festgestellt werden. Interessanterweise beinhalteten alle diese Dateien im Dokumentenname das Wort «russisch». («InfoblattRussisch.docx»): Es scheint, als ob diese Dokumente gezielt (ev. automatisiert) aus dem geleakten-Dump entfernt wurden. In einem der fünf Haupt-Kundenprojekte sind viele Unterverzeichnisse und Dateien nicht veröffentlicht worden. Dabei handelt es sich um Verzeichnisnamen wie «Realisierung, Test, Installation, Dokumentation, Abnahme, Images, Adressbücher, Architektur, Berechtigungen, Codegruppen, Domains PKI Mailer, usw. Ob diese bewusst von Play nicht veröffentlicht wurden ist kaum abschätzbar.
- Armasuisse / Militärpolizei: Der Datenbestand im Umfang von 2.3GB umfasste 1903 Dateien und 586 Ordner. Die Analyse erfolgte durch FUB/milCERT mit folgendem Ergebnis: Nicht veröffentlicht wurden insbesondere detaillierte Offerten (inkl. Ausschreibungsunterlagen), Rechnungen und Verträge. Zusätzlich wurden auch Dokumente zu Deployment-Tests nicht veröffentlicht. Es ist keine Systematik zu erkennen. Es könnte auch gut technisch bedingt am Kopiervorgang gelegen haben, bei dem gewisse Ordner respektive Dateien nicht mitkopiert wurden.
- Die Auswertung des NCSC zu den Datenbeständen des BJ, ISC-EJPD, SEM und BAZG ergab folgendes Ergebnis:

Dateien	**BJ**	**ISC-EJPD**	**SEM**	**BAZG**
Gesamt	26'719 (100%)	16'961 (100%)	178 (100%)	30'757 (100%)
Veröffentlicht	6'325 (24%)	4'768 (28%)	3 (2%)	7'067 (23%)
Nicht veröffentlicht	20'394 (76%)	12'193 (72%)	175 (98%)	23'690 (77%)

Die Mehrheit der bei Xplain vorhandenen Datenbeständen der VE wurden nicht veröffentlicht. Anhand von Stichproben wurde der nicht veröffentlichte Datenbestand geprüft und der Inhalt dieser Dokumente gesichtet. Es ist keine Systematik erkennbar, nach welcher einzelne Datenbestände zurückbehalten und nicht veröffentlicht wurden. Es ist wahrscheinlich, dass die Auswahl der veröffentlichten Daten aus technischen Gründen oder aufgrund limitierter Ressourcen (Zeit, Netzwerk-Bandbreite) der Täterschaft erfolgte.

7.2 Einschätzung NCSC

Das Vorgehen der Täterschaft, Dokumente mit der Bezeichnung «InfoblattRussisch.docx» aus dem Datenbestand von fedpol zu entfernen, scheint zwar einer gewissen Systematik zu folgen, deutet aber eher darauf hin, dass sich die Täterschaft dadurch selbst schützen will. Es ist von anderen Cyberkriminellen-Gruppierungen aus Russland bekannt, dass diese einen Bezug zu Russland vermeiden, um nicht Gefahr zu laufen, in den Fokus der eigenen Behörden zu geraten. Bei diesem Dokument handelt sich um ein auf Russisch verfasstes Informationsblatt für festgenommene Personen (Rechte und Pflichten, Ablauf, usw.) ohne sensitiven Inhalt. Dasselbe Dokument existiert in verschiedenen weiteren Sprachen im veröffentlichen Datenbestand. Eine weiterführende Analyse hat ergeben, dass das Dokument «InfoblattRussisch.docx» nur dann aus dem Datenbestand entfernt wurde, wenn es nicht in einem Archiv (z. B. einer .zip-Datei) enthalten und dadurch einfach auffindbar war. Dieses Vorgehen deutet auf eine oberflächliche Prüfung des Datenbestands ohne inhaltliche Sichtung durch die Täterschaft hin.

Dem NCSC liegen keine Hinweise vor, dass die Gruppierung Play bei der Veröffentlichung von Datenlecks anderer betroffenen Firmen oder Organisationen spezifische Daten zurückbehalten hätte. Ebenfalls hat eine oberflächliche und Stichprobenprüfung der verschiedenen durch Play veröffentlichten Leaks ergeben, dass die Gruppierung bereits in anderen Fällen falsche oder ungenaue Grössenangaben zu den Datenbeständen publiziert hat.
Anhand der Delta-Analyse des Datenbestands konnten somit keine Hinweise gefunden werden, dass Daten bewusst zurückgehalten wurden. Das NCSC geht daher davon aus, dass keine weiteren Veröffentlichungen drohen. Es gibt zudem auf Grund der Analyse keine Hinweise darauf, dass die Kriminellen Teile des Datenbestands anderweitig weitergegeben haben.

8 Fazit aus den Datenanalysen

Bei einem Cyberangriff, welcher zu einem Abfluss von Daten führt, stellt sich für Betroffene nicht mehr nur die Frage, wie der operative Betrieb wiederaufgenommen werden kann, sondern auch, welche Auswirkungen der Verlust der Daten hat. Diese Fragen sind für den Bund besonders wichtig, da diese die entsprechenden Daten im öffentlichen Auftrag bearbeitet. Im Fall des Cyberangriffs auf die Firma Xplain stellten sich diese Fragen noch drängender, weil es sich um einen IT-Dienstleister im Bereich der inneren Sicherheit handelt und damit sehr sensible Daten betroffen waren.
Im Bericht wurde aufgezeigt, dass für die Beantwortung der Frage, welche Daten von wem in welchem Ausmass abgeflossen sind, bereits einen beträchtlichen Analyseaufwand nötig machen. Unstrukturierte Datensätze müssen zunächst mit Hilfe von geeigneten Instrumenten aufbereitet und lesbar gemacht werden. Anschliessend führt bei den als relevant identifizierten Daten kein Weg an einer manuellen Sichtung und Kategorisierung vorbei. Das ist bei grossen Datenmengen ein hoher Aufwand, der viel Zeit und Personalressourcen in Anspruch nimmt.
Eine umfassende Datenanalyse ist aber zwingend notwendig, um den Vorfall wirklich beurteilen zu können. Wenn dieser Prozess nicht durchgeführt wird, bleibt unklar, wer wirklich in welchem Ausmass betroffen ist und das Risiko, dass relevante Daten veröffentlicht sind, ohne, dass dies den Betroffenen klar ist, bliebe zu gross. Selbstverständlich ist die umfassende Datenanalyse auch eine wichtige Voraussetzung für die Aufarbeitung des Vorfalls. Die dafür relevanten Erkenntnisse werden im Rahmen der angeordneten Administrativuntersuchung aufgearbeitet.

Wie bei vielen Krisensituationen war zur Durchführung der Datenanalyse viel Improvisation nötig. Das NCSC kann aber feststellen, dass es in relativ kurzer Zeit gelungen ist, die nötigen Infrastrukturen und Personalressourcen bundesintern zu mobilisieren. Dank den Datenanalysen und der engen Zusammenarbeit mit allen Betroffen konnte das NCSC die politische Führung und die Öffentlichkeit so transparent wie möglich informieren.
Leider ist trotzt allen Vorsichtsmassnahmen damit zu rechnen, dass es auch künftig zu Vorfällen kommt, bei denen Daten des Bundes betroffen sind. Es wird wichtig sein, dass in der Bundesverwaltung die Zuständigkeiten geklärt und die operativen Fähigkeiten weiter ausgebaut werden, um Daten rasch und umfassend zu analysieren.